**Лабораторна робота 9. Системи з відкритим ключем. Криптосистема RSA.**

**Тема роботи: Системи з відкритим ключем. Криптосистема RSA.**

**Ціль роботи: Відпрацювати вміння використання криптосистеми RSA. На практиці зашифрувати текст за допомогою цього алгоритму шифрування.**

**Загальні відомості**

Концепцію систем з відкритим ключем запропонували у 1976 році Діффі і Хеллман.[19] Криптосистеми з відкритим ключем засновуються на використанні особливих властивостей шифрування, що являє собою розрахунок оберненої величини від якоїсь функції, що не може бути реалізована числовими методами.

В сучасній криптографії стандартом де-факто на системи з відкритим ключем є система RSA, спроектована Рівестом, Шаміром та Адлеманом [2].

**Теоретичні відомості**

Розглянемо математичні результати, покладені в основу алгоритму RSA.

*Теорема 1. (Мала теорема Ферма.)*

Якщо р – просте число, то

*xp-1 = 1 (mod p)* (1)

для будь-якого *х*, простого відносно р, і

*xp = х (mod p)* (2)

для будь-якого *х.*[1]

*Визначення. Функцією Эйлера* *ϕ(n)* називається число позитивних цілих, менших *n* і простих відносно *n*.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *n* | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| *ϕ(n)* | 1 | 2 | 2 | 3 | 2 | 6 | 4 | 6 | 4 |

*Теорема 2.* Якщо *n*=*pq*, (*p* і *q* – відмінні друг від друга прості числа), то

*ϕ(n)=(p-1)(q-1).*

*Теорема 3.* Якщо *n*=*pq*, (*p* і *q* – відмінні друг від друга прості числа) і *х* – просте відносно *р* и *q*, то

*xϕ(n) = 1 (mod n).*

*Наслідок .* Якщо *n*=*pq*, (*p* і *q* – відмінні друг від друга прості числа) і є просте відносно *ϕ(n),* то відображення

*Ее,n: x→xe (mod n)*

є взаємно однозначним на **Z**n.

Очевидний і той факт, що якщо *е* – просте відносно (*n*), то існує ціле *d*, таке, що

*ed = 1 (mod ϕ(n))* (3)

На цих математичних фактах і заснований популярний алгоритм RSA.[4]

Нехай *n*=*pq*, де *p* і *q* – різні прості числа. Якщо *e* і *d* задовольняють рівнянню (3), то відображення Ее,n і Еd,n є інверсіями на Zn. Як Ее,n, так і Еd,n легко розраховуються, коли відомі *e*, *d*, *p*, *q*. Якщо відомі *e* і *n*, але *p* і *q* невідомі, то Ее,n являє собою однобічну функцію; перебування Еd,n по заданому *n* рівнозначно розкладанню *n*. Якщо *p* і *q* – досить великі прості, то розкладання *n* практично не здійсненне. Це і закладено в основу системи шифрування RSA.

*Користувач i* вибирає пару різних простих *p*i і *q*i і розраховує пари цілих *(ei, di)*, що є простими відносно *ϕ(ni)*, де *n*i=*p*i *q*i . Довідкова таблиця містить публічні ключі *{(ei ,ni)}*.[20]

Припустимо, що вихідний текст

*x =(x0, x1, ..., xn-1), x∈Zn , 0 ≤ i < n,*

Zn-безліч цілих чисел

спочатку представлений по підставі *n*i :

*N = c0+ci ni+....*

Користувач *i* зашифровує текст, при передачі його користувачу *j*, застосовуючи до *n* відображення E*di,ni* :

*N → Edi,ni n = n’.*

Користувач *j* робить розшифрування *n*’, застосовуючи E*ei,ni* :

*N’ → Eei,ni n’= Eei,ni Edi,ni n = n .*

Очевидно, для того щоб знайти інверсію E*di,ni* стосовно E*ei,ni*, потрібно знання множників *n*=*p*i *q*i. Час виконання найкращих з відомих алгоритмів розкладання при *n*=10100 на сьогоднішній день виходить за межі сучасних технологічних можливостей [1].

Розглянемо кілька прикладів, що ілюструють застосування алгоритму RSA.

**Приклад 1**Зашифруємо повідомлення “САВ”. Для простоти будемо використовувати маленькі числа (на практиці застосовуються набагато більші).

Виберемо p=3 і q=11.

Визначимо n=3\*11=33.

Знайдемо (p-1)(q-1)=20. Отже, у якості d, взаємно простої з 20, приймемо наприклад, d=3.

Виберемо число е. Як таке число може бути узяте будь-яке число, для якого задовольняється співвідношення (е\*3) (mod 20) = 1, наприклад 7.

Примітка: для простого знаходження числа *е* досить вирішити в цілих числах рівняння  , де *а*=1,2..*n* (перебираючи значення *n* до першого цілого *е*)

Представимо повідомлення як послідовність цілих чисел за допомогою відображення: А→1, У→2, З→3. Тоді повідомлення приймає вид (3,1,2). Зашифруємо повідомлення за допомогою ключа {7,33}.

C[1] = (37) (mod 33) = 2187 (mod 33) = 9,

C[2] = (17) (mod 33) = 1 (mod 33) = 1,

C[3] = (27) (mod 33) = 128 (mod 33) = 29.

Розшифруємо отримане зашифроване повідомлення C{9,1,29} на основі закритого ключа {3,33}:

M[1] = (93) (mod 33) = 729 (mod 33) = 3,

M[2] = (13) (mod 33) = 1 (mod 33) = 1,

M[3] = (293) (mod 33) = 24389 (mod 33) = 2.

Приклад 2

Шифруємо слово БІГ . Коефіцієнти *p*=3, *q*=7.

Визначимо *n*=*p\*q=*3\*7=21. Знайдемо *(p-1)(q-1)*=12. Виберемо *d* = 5. Знайдемо число *е*, для якого справедливо

*ed mod ((p-1)(q-1))* = 1.(вирішуємо рівняння  де *а*=1,2...*n*;) виберемо з безлічі рішень відмінне від числа *d* число, *е* = 17.

Представимо шифруєме слово у вигляді послідовності чисел 2 6 4 (порядковий номер букв у алфавіті)

Шифрування по відкритому ключу (17,21):

C1=217 mod(21) = 131032 mod (21) =11;

C2 = 617mod (21) = 16926659444736 mod (21) = 6;

C3 = 417mod(21) = 17179869184 mod (21) = 16.

Отримане зашифроване повідомлення :11 6 16.

Розшифруємо зашифроване повідомлення по секретному ключу (5,21)

М1= 115mod (21) = 161051 mod (21) = 2;

M2 = 65 mod (21) = 7776 mod (21) = 6;

M3 = 165 mod (21) = 1048576 mod (21) = 4.

У підсумку одержуємо вихідне повідомлення БІГ.

Отже, у реальних системах алгоритм RSA реалізується в такий спосіб: кожен користувач вибирає два великих простих числа, і від­повідно до описаного вище алгоритма вибирає два простих числа *e* і *d*. Як результат множення перших двох чисел (*p* і *q*) установлюється *n*.

*{e,n}* утворить відкритий ключ, а *{d,n}* – закритий (хоча можна взяти і навпаки).

Відкритий ключ публікується і доступний кожному, хто бажає послати власнику ключа повідомлення, що зашифровується зазначеним алгоритмом. Після шифрування, повідомлення неможливо розкрити за допомогою відкритого ключа. Власник же закритого ключа легко може розшифрувати прийняте повідомлення [20].

Особливості методу накладають деякі обмеження на значення деяких змінних. *Наприклад*: змінна D повинна бути взаємно простою відносно M, тобто ці числа не повинні мати спільних дільників, а змінна E повинна бути такою, щоб залишок від ділення (D\*E) на M дорівнював 1.

**Порядок виконання лабораторної роботи**

1. Повідомлення шифрується вручну посимвольно з використанням алфавіту: \_АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ
2. Після ручного шифрування для перевірки результату необхідно розшифрувати отриманий шифртекст (також посимвольно).